UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/939,233	08/24/2001	Ray Frankulin	019411-001410US	3401

20350 7590 08/14/2009

TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER	
MCCLELLAN, JAMES S	

ART UNIT	PAPER NUMBER
3714	

MAIL DATE	DELIVERY MODE
08/14/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte RAY FRANKULIN and STAN JONES

Appeal 2009-003516
Application 09/939,233
Technology Center 3700

Decided: August 14, 2009

Before DONALD E. ADAMS, DEMETRA J. MILLS, and ERIC GRIMES, *Administrative Patent Judges*.

MILLS, *Administrative Patent Judge*.

DECISION ON APPEAL

STATEMENT OF CASE

This is a decision on appeal under 35 U.S.C. § 134 from the Examiner's final rejection of claims 1-17. The Examiner has rejected the claims for obviousness. We have jurisdiction under 35 U.S.C. § 6(b).

Claim 1 is representative of the subject matter on appeal and reads as follows:

1. A method employing a location verifier system for verifying that a user is located within a predefined geographical area, after which the user is allowed to place a telephone wager on a sports book, the method comprising:

receiving by the location verifier system, a telephone call from the user requesting access to the sports book;

forwarding a verification number to the user, the verification number being received by the user only if the user is located within the predefined geographical area;

receiving the verification number from the user;

verifying the verification number forwarded is the same verification number received; and

permitting the user to place the telephone wager on the sports book.

Cited References

Seheidt et al. (Seheidt)	US 5,787,173	July 28, 1998
LaDue	US 5,999,808	Dec. 7, 1999
Wicks	US 6,011,485	Jan. 4, 2000
Paravia et al. (Paravia)	US 6,508,710 B1	Jan. 21, 2003

Grounds of Rejection

1. Claim 1 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Paravia in view of Seheidt.
2. Claims 2-17 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Paravia in view of Seheidt, further in view of Wicks or LaDue.

ISSUE

The Examiner argues that:

> While Paravia teaches the use of various techniques for granting the user access to the sports wagering game (col. 2, lines 11-12), Paravia is silent regarding the feature of receiving and transmitting a verification number to and from the user in order to allow play. As indicated in the initial office action, this feature is known in cryptographic verification systems as a handshaking process. In an analogous system of verification of user identity, Seheidt teaches a handshaking system in which there is transmission and reception of verification information {cryptographic key data} from a remote site to a user and back from a user (abstract; Fig. 1). It would have been obvious to a person of ordinary skill in the art at the time of the invention to enhance the verification/authorization system of Paravia, by sending and receiving the password verification number of Paravia in a handshaking manner, as disclosed by Seheidt, in order to make gaming more secure.

(Ans. 3-4.)

Appellants contend that Seheidt sends two different key components. (App. Br. 6.)

The main issue is: Have Appellants demonstrated error in the Examiner's obviousness rejection; particularly, does the combination of Paravia and Seheidt disclose a step of "verifying the verification number forwarded is the same verification number received."

FINDINGS OF FACT

1. According to the Specification, page 3,

> A control center is contacted by the user and then generates a verification number. The control system then contacts the pager, and

> provides the verification number to the user via the pager. The user then inputs the verification number to the control center, which then provides access to the system to the user.

2. According to the Specification, page 3, the invention includes a step of verifying that the verification number forwarded to the user is the same verification number received from the user.

3. Seheidt discloses that:

> For two people to communicate securely using conventional cryptography, those two persons must not only possess compatible cryptographic equipment, they must also have identical keys. Further, those keys must be kept secret from anyone not in a position of confidence with the two communicators and must be changed periodically to guard against compromise. In addition to the protection of the keys themselves, selecting the proper key sequence and increasing the frequency with which the key sequence is changed can enhance the security of this type of protection. The function of key management is the process of generating, distributing, changing, replacing, storing, checking on and destroying cryptographic keys.

(Col. 1, l. 65 to col. 2, l. 12.)

4. Seheidt discloses that its cryptographic key management system is "for the secure communication of a message from a transmitting user to a receiving user using a split key scheme. The message may be in voice, data or any other signal in digital form." (Col. 4, ll. 19-23.)

5. Seheidt discloses that "once a match is established a both locations, the transmit key component and the receive key component … are combined at both locations, forming identical complete keys at both locations. (Col. 4, ll. 51-54.)

6. Seheidt discloses that the identical complete keys are then used to initiate the cryptographic engines at both locations for subsequent encryption and decryption of messages between the two locations. (Col. 4, ll. 61-67.)

7. Seheidt, Figs. 3a and 3b, show a flow diagram of the Seheidt method and show that only split key components are transmitted from the transmitting user to the receiving user, and the full key is not transmitted but used only for encryption purposes.

PRINCIPLES OF LAW

"In rejecting claims under 35 U.S.C. § 103, the examiner bears the initial burden of presenting a prima facie case of obviousness. Only if that burden is met, does the burden of coming forward with evidence or argument shift to the applicant." *In re Rijckaert*, 9 F.3d 1531, 1532 (Fed. Cir. 1993) (citations omitted). In order to determine whether a prima facie case of obviousness has been established, we consider the factors set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 17 (1966): (1) the scope and content of the prior art; (2) the differences between the prior art and the claims at issue; (3) the level of ordinary skill in the relevant art; and (4) objective evidence of nonobviousness, if present.
Each element claimed must be found in the prior art.

ANALYSIS

Appellants argue that Seheidt sends two different key components and thus does not transmit the same key, as claimed. (App. Br. 6.)

We are persuaded by Appellants' argument. Seheidt discloses that its cryptographic key management system is for the secure communication of a message from a transmitting user to a receiving user using a split key scheme. (Col. 4., ll. 19-23.) Seheidt discloses that "once a match is established a both locations, the transmit key component and the receive key component … are combined at both locations, forming identical complete keys at both locations. (Col. 4, ll. 51-54.)

However, Seheidt discloses that the identical complete keys are used to initiate the cryptographic engines at both locations for subsequent encryption and decryption of messages between the two locations. (Col. 4, ll. 61-67.) Seheidt Figs. 3a and 3b show a flow diagram of the Seheidt method and show that only split key components are transmitted from the transmitting user to the receiving user, and the full key is not transmitted but used only for encryption purposes. (FF7.) Thus, Seheidt's method does not include a step in which one party forwards a verification number to the other party, and receives back the same verification number from the other party.

CONCLUSION OF LAW

Appellants have demonstrated error in the Examiner's obviousness rejection; particularly, the combination of Paravia and Seheidt does not disclose a step of "verifying the verification number forwarded is the same verification number received."

The obviousness rejection is reversed.

Appellants present similar arguments to the rejection of claims 2-17 over Paravia in view of Seheidt, further in view of Wicks or LaDue as presented for the rejection of claim 1. (Br. 7.) Therefore, for the same reasons given herein with respect to the rejection of claim 1, we reverse the rejection of claims 2-17.

SUMMARY

Each of the obviousness rejections under 35 U.S.C. § 103(a) is reversed.

REVERSED

clj

TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834